EXHIBIT B

Ekwan E. Rhow - State Bar No. 174604
erhow@birdmarella.com
Marc E. Masters - State Bar No. 208375
mmasters@birdmarella.com
BIRD, MARELLA, RHOW,
LINCENBERG, DROOKS, & NESSIM, LLP
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Jonathan M. Rotter - State Bar No. 234137
jrotter@glancylaw.com
David J. Stone - State Bar No. 208961
dstone@glancylaw.com
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
Email: info@glancylaw.com

Korey A. Nelson (admitted *pro hac*)
knelson@burnscharest.com
Amanda K. Klevorn (admitted *pro hac*)
aklevorn@burnscharest.com
Claire Bosarge Curwick (admitted *pro hac*)
ccurwick@burnscharest.com
Logan B. Fontenot (admitted *pro hac*)
lfontenot@burnscharest.com
BURNS CHAREST LLP
365 Canal Street, Suite 1170
New Orleans, LA 70130
Telephone: (504) 799-2845

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CHRISTOPHER KARWOWSKI, MELODY KLEIN, MICHAEL MCBRIDE, and AIMEN HALIM, individual and on behalf of all others similarly situated,

Plaintiffs,

vs.

GEN DIGITAL INC., a corporation, et al.,

Defendants.

CASE NO. 3:22-cv-08981-RFL

DECLARATION OF ATIF HASHMI IN SUPPORT OF PLAINTIFFS' OPPOSITION TO DEFENDANT GEN DIGITAL'S MOTION FOR ATTORNEYS' FEES

DECLARATION OF ATIF HASHMI

I, Atif Hashmi, declare as follows:

1. I am the President and Chief Scientist of Bitwise Forensics Research, Inc., which provides engineering consulting services. My clients have included large computer and technology companies, as well as smaller companies and startups. I am fully familiar with the facts contained herein based upon my personal knowledge, analysis, and upon information provided by Plaintiffs' counsel, and if called as a witness, I could and would testify competently thereto. I submit this declaration at the request of Plaintiffs' counsel in connection with the above-captioned action (the "Action").

2. I hold a B.S. in Computer Engineering from Lahore University of Management Sciences ("LUMS") in Pakistan. I also hold an M.S. and Ph.D. in Electrical Engineering from the University of Wisconsin in Madison, Wisconsin. My educational training and research have been focused on software engineering, computer architecture, machine learning, operating systems, and design and development of hardware circuits and software for computing systems. I have more than 20 years of experience in software design and development for distributed systems, embedded devices, server-client based systems, mobile platforms, operating systems, neural networks, and machine learning based platforms. I have studied and developed software using programming languages including C, C++, Java, Python, JavaScript, Embedded C, Assembly Language, PHP, and others.

3. I have published research papers related to machine learning, artificial intelligence, computer hardware, and software in peer-reviewed computer science and electrical engineering conferences. Several of these publications have received best research paper awards. I have been an invited speaker at venues including academic conferences and

technology companies. I have been an expert due-diligence panelist for the National Science Foundation to evaluate proposal submitted to NSF in the areas of sensor-based systems and machine learning. I am a named inventor on patents and patent applications for neural network software and hardware for processing sensory data. A complete list of patents and patent applications on which I am a named inventor is included in my CV, attached hereto as **Exhibit 1**.

4. Over the years, I have consulted in over 100 legal matters involving software copyright infringement, privacy, trade secret theft, source code quality, and patent infringement. I have given testimony as an expert and submitted reports in which I offered opinions regarding my technical analysis. As a technical expert, I have reviewed thousands of lines of source code developed in several programming and hardware descriptive languages including C/C++, Java, JavaScript, Ruby, SQL, and Verilog-HDL. Additional details about specific cases can be found in my CV attached as Exhibit 1.

5. I am being compensated at a rate of $700 per hour in connection with this declaration.

6. This declaration is based on information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study, and thus may expand or modify my opinions as my investigation and study continues. I also reserve the right to supplement my opinions in response to any additional information that becomes available to me, any matters raised by Defendant and/or opinions rendered by Defendant's experts, or in light of any relevant orders from the Court.

I. Plaintiffs' allegations have been reasonable from a technological standpoint.

7. It is my understanding that Plaintiffs have alleged that Gen Digital invaded their privacy by, among other things, using the Avast Online Security and Privacy browser extension ("AOSP") to embed third party advertising cookies in web traffic between AOSP and Defendant's servers so that AOSP users' web browsing data could be stored on Defendant's servers along with their third party cookie data before being linked together to create detailed profiles of AOSP users that Defendant ultimately sold to third party advertisers for profit.[1]

8. Defendant's Motion omits important information about how cookies are inserted in transmissions from a browser to certain servers.[2] Browsers *can* append cookie data to transmissions to the related servers.[3] However, Defendant ignores the critical role browser extensions play in specifying whether any cookie data is included in transmissions from a browser to certain servers—in particular, the servers associated with the extension, here the server hosting the urlite.ff.avast.com domain associated with the AOSP extension.

9. Browsers, by default, may "automatically [] append[]" cookie data to a user's browsing data and transmit the browsing data appended with the cookies data to *certain* servers. However, once a browser extension, like AOSP, is installed on the user's browser, it is not necessarily true that the browser will continue to "automatically [] append[]" cookie data to a user's browsing data as it did in the default scenario, particularly as to the servers associated with the extension. Instead, browser extensions can change the default behavior

[1] *See* ECF No. 47, Plaintiffs' First Amended Complaint, ¶¶ 70-134.
[2] *See* ECF No. 140-2, Defendant's Corrected Notice of Motion and Motion for Attorneys' Fees, pp. 4-8.
[3] *See id.*

of a browser by specifying whether any cookie data is to be transmitted to the extension-related servers along with users' browsing data. In other words, browser extensions, including AOSP, can control the behavior of a browser and can specify whether the browser should append cookie data to users' browsing data within the transmissions sent to the extension-related servers.

A. One Way to Control Cookie Transmission: The *Credentials* Parameter

10. One way a browser extension may specify whether cookie data is embedded in transmissions to certain servers is through the *credentials* parameter of the *fetch* API.[4] The *fetch* API provides a JavaScript interface that allows browser extensions to send requests to certain servers and process the responses sent by the servers.[5] The *credentials* parameter of the *fetch* API controls whether or not the browser sends credentials, which include cookie data, to certain servers. The *credentials* parameter of the fetch API can take one of the following three values:[6]

a. *omit*: never send credentials.

b. *same-origin*: only send credentials for same-origin requests.

c. *include*: always include credentials, even cross-origin.

11. If the *credentials* parameter is set to *omit*, the browser will not send the cookie data and any other credential information along with the users' browsing data within transmissions to the browser extension's related servers.[7] If the *credentials* parameter is set to *same-origin* (which is the default parameter if not expressly set to something else), or if

[4] *See* https://developer.mozilla.org/en-US/docs/Web/API/Fetch_API/Using_Fetch
[5] *See id.*
[6] *See id.*
[7] *See id.*

a browser extension does not specify the value of the *credentials* parameter while using the *fetch* API, the browser may by default send the cookie data and any other credential information (if present) along with the users' browsing data within transmissions to extension related servers.[8] And if the credentials parameter is set to *include*, the browser may send the cookie data and other credentials information to extension related servers and non-extension related servers.[9] Thus, by using the *credentials* parameter of the *fetch* API, browser extensions can control the behavior of a browser and can specify whether the browser appends cookie data to the users' browsing data within the transmissions sent to extension related servers, including the urlite.ff.avast.com server to which the AOSP extension sends browsing data and cookies data.

12. Accordingly, Defendant's claim that the AOSP extension does not control whether cookies are sent to Defendant's servers is incorrect.

13. To show how AOSP configured the *credentials* parameter, I installed the currently available AOSP version 22.12.6 released on September 2, 2024, from the Google Chrome Store ("September 2024 AOSP").[10] Using the DevTools analysis tool that comes pre-installed within the Google Chrome browser,[11] I extracted the AOSP source code contained within the *background.js* file. The *background.js* file implements the *handleRequest* function that transmits a URL accessed by the browser to Defendant's servers

[8] *See id.*
[9] *See id.*
[10] *See* https://chromewebstore.google.com/detail/avast-online-security-pri/gomekmidlodglbbmalcneegieacbdmki.
[11] *See* https://developer.chrome.com/docs/devtools.

for further analysis. I provide a screen capture of the source code that implements the *handleRequest* function in Figure 1.

```
40441     handleRequest() {
40442       return __async(this, null, function* () {
40443         this.validateUrl();
40444         try {
40445           const response = yield fetch(this.getResolvedUrl(), this.getOptions());
40446           yield this.onCompleted(response);
40447         } catch (e) {
40448           this.reject(new LoaderError(e));
40449         }
40450       });
40451     }
```

Figure 1: Implementation of the AOSP's *handleRequest* function.

14. As shown in Figure 1, the *handleRequest* function, at line 40445, utilizes the *fetch* API to send the URL accessed by the browser to Defendant's servers. The *fetch* API, subsequently, at line 40445, calls the *getOptions* function to obtain the configuration parameters for the *fetch* API. I provide a screen capture of the source code that implements the *getOptions* function in Figure 2.

```
29566     getOptions() {
29567       const options = {
29568         headers: this.headers,
29569         method: this.method,
29570         signal: this.controller.signal
29571       };
29572       if (this.body)
29573         options.body = this.body;
29574       return options;
29575     }
```

Figure 2: Implementation of the AOSP's *getOptions* function.

15. As shown in Figure 2, the *getOptions* function does not explicitly set the *credentials* parameter. As discussed earlier, for this situation, the *fetch* API will use the default value of the *credentials* parameter, which is set to *same-origin*, and will enable the browser to send credentials, including the cookie data, for same-origin requests. By instead setting the *credentials* parameter to *omit* within the *getOptions* function, AOSP could cause

the browser to not send any credential data, including the cookies data, to Defendant's servers.

16. In other words, Defendant chose not to set the *credentials* parameter to *omit*, and, therefore, programmed AOSP in a manner that enables the browser to send cookies data to the Defendant's servers.

17. I performed further testing of the September 2024 AOSP to determine whether modifying the corresponding source code in the ways I have described here can disable the browser from including cookies data in transmissions to Defendant's servers.

18. To determine whether cookie data is included within the transmissions by AOSP to the Defendant's servers when the *credentials* parameter is set to *omit* within the September 2024 AOSP, using the DevTools analysis tool I made changes to the source code of the September 2024 AOSP as shown in Figure 3.

```
29566     getOptions() {
29567       const options = {
29568         headers: this.headers,
29569         method: this.method,
29570         credentials: 'omit',
29571         signal: this.controller.signal
29572       };
29573       if (this.body)
29574         options.body = this.body;
29575       return options;
29576     }
```

Figure 3: Implementation of the AOSP's *getOptions* function with *credentials* parameter set to *omit*.

19. I captured the network traffic before and after making the changes to the source code of the September 2024 AOSP as shown in Figure 3. As shown in Figure 4 and Figure 5, my network traffic analysis confirmed that before making the changes to the source code of the September 2024 AOSP, cookie data was included within the transmission sent by AOSP to Defendant's servers and after making the changes to the source code of the

September 2024 AOSP, cookie data was not included within the transmission sent by AOSP to Defendant's servers. This further shows that by setting the *credentials* parameter to *omit* within the *getOptions* function, AOSP can cause the browser to not send any cookie data to Defendant's servers.

Figure 4: Transmission to Defendant's servers without setting the *credential* parameter to *omit* that includes cookie data.

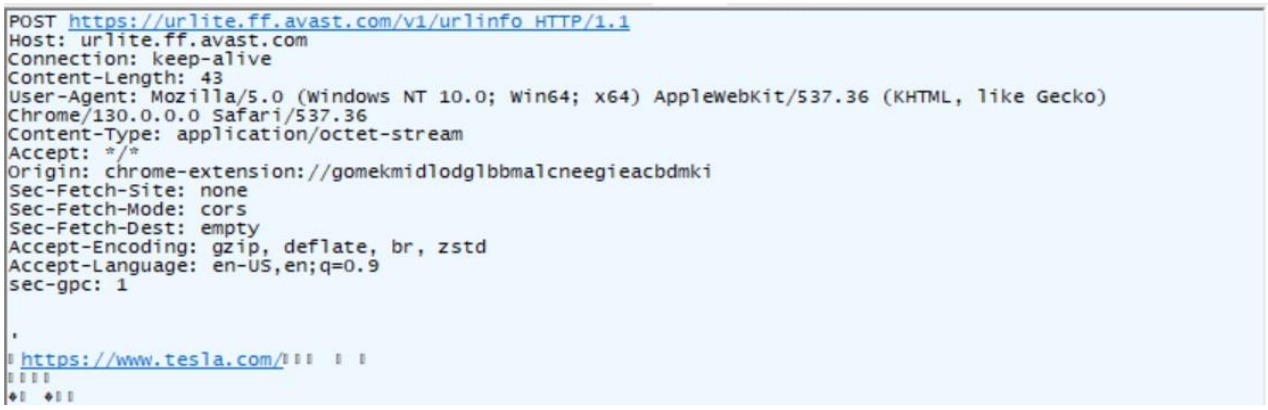

Figure 5: Transmission to Defendant's servers with setting the *credential* parameter to *omit* that does not include cookie data.

B. Another Way to Control Cookie Transmission: The Set-Cookie Header

20. Another way by which servers can control the behavior of the browsers with respect to transmission of the cookie data is by using the *Set-Cookie* header. In my previous

declaration, I also explained that the results of my experiments during this litigation have run "[c]ontrary to Defendant's assertion that the browser, not [Defendant], is responsible for embedding the cookies in the network traffic" transmitted to Defendant's servers.[12] In that declaration, I described that cookie data is appended to the transmission to Defendant's servers via the urlite.ff.avast.com subdomain. Specifically, based on my analysis and review of the network traffic between the AOSP Client Device and Defendant's servers, I determined that the AOSP Client Device, at various times sent the following cookies from third-party companies bearing the corresponding cookie identifiers to Defendant's servers: (i) Adobe Inc.: AMCV_, AMCVS_, and s_nr, ;[13] (ii) Alphabet Inc.: _ga, _gcl_au, and _gid;[14] (iii) META Platforms Inc.: _fbp;[15] (iv) Microsoft Corporation: _uetvid;[16] and (v) Reddit, Inc.: _rdt_uuid.[17] An example of data sent by an AOSP Client Device to Defendant's servers

[12] *See* ECF No. 97-2, Declaration of Atif Hashmi in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45, ¶ 10.
[13] *See Cookies and the Experience Cloud Identity Service*, Adobe Experience League, (Aug. 23, 2024), https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies; *see also Adobe plug-in: getNewRepeat*, Adobe Experience League, (Aug. 23, 2024), https://experienceleague.adobe.com/en/docs/analytics/implementation/vars/plugins/getnewrepeat.
[14] *See How Google Uses Cookies*, Google Privacy & Terms, (Aug. 23, 2024), https://policies.google.com/technologies/cookies?hl=en-US; *see also Our advertising and measurement cookies*, Google, (Aug. 23, 2024), https://business.safety.google/adscookies/.
[15] *See ClickID and the fbp and fbc Parameters*, Meta for Developers, (Aug. 23, 2024), https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/.
[16] *See FAQ: Universal Event Tracking*, Microsoft Ads Help, (Aug. 26, 2024), https://help.ads.microsoft.com/apex/index/3/en/53056/.
[17] *See Cookie Policy*, Super Metrics Cookie Policy, (Aug. 26, 2024), https://supermetrics.com/cookie-policy; Also see *LinkedIn Cookie Table*, LinkedIn Legal, (Aug. 26, 2024), https://www.linkedin.com/legal/l/cookie-table.

is shown in **Figure *6***.

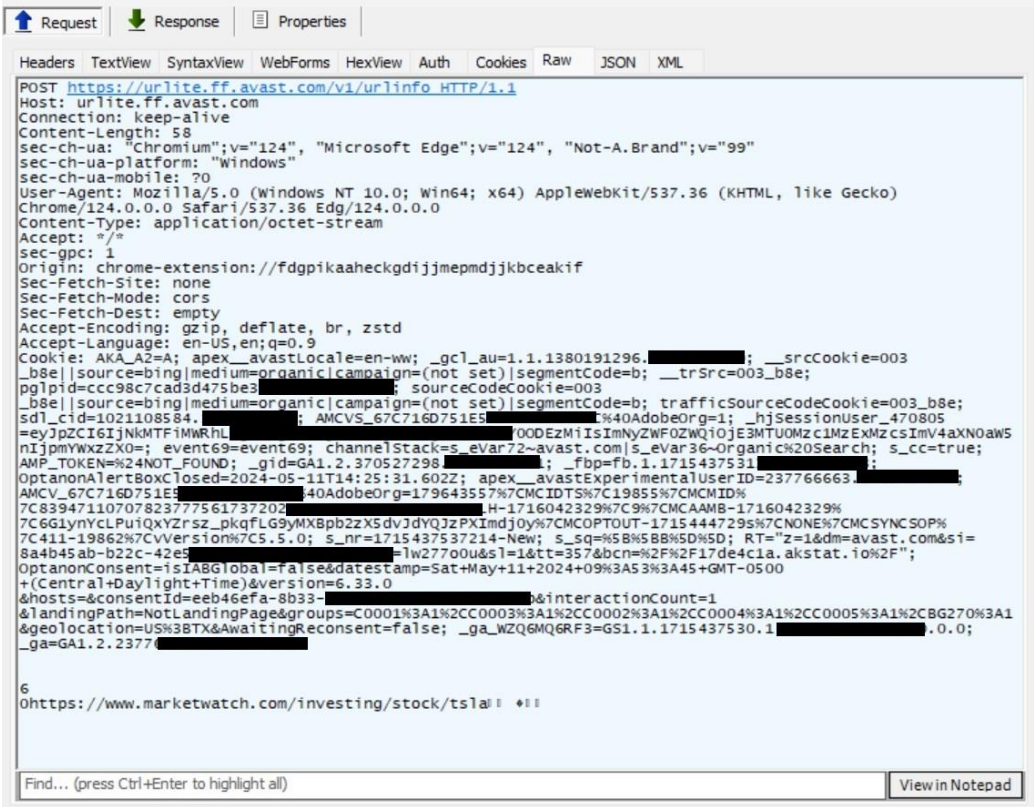

Figure 6: Data including URL and Cookie Identifiers sent by the AOSP Client Device to Defendant's servers.

21. Cookies and corresponding cookie identifiers are appended to the transmission to Defendant's servers sent to the urlite.ff.avast.com subdomain, because the cookies set by avast.com at the outset of the process are configured in a way to allow those cookies to be sent to Avast's servers via the urlite.ff.avast.com subdomain. More specifically: a server can send the *Set-Cookie* header to set up or install a cookie on a user's device. That is what Avast's servers do when the AOSP Client Device accesses https://www.avast.com. Within the *Set-Cookie* headers, the Domain and Path attributes define the scope of a cookie, i.e., what servers the cookies are sent to. If the *Set-Cookie* header does not specify/include a Domain attribute, the cookies are transmitted to the server that sets it but not to the servers

associated with subdomains.[18] Based on my testing in May 2024, as shown in **Figure 7**, for certain cookies Defendant specifically set the Domain attribute in a way that causes the cookies to be sent to the Defendant's servers via the urlite.ff.avast.com subdomain. Defendant could have configured the *Set-Cookie* headers such that cookies and corresponding cookie identifiers are not sent to Defendant's servers via the urlite.ff.avast.com subdomain.

Figure 7: Response from Avast's servers showing that the domain element of Set-Cookie header is set to avast.com (May 2024).

22. Thus, my experiments showed that Defendant could have configured the *Set-Cookie* header such that the browser would not have sent cookies back to Defendant servers via the urlite.ff.avast.com subdomain along with users' browsing data.[19] I understand that Defendant now justifies this by arguing that the cookies "are designed to be used in connection with www.avast.com and also various subdomains involved in the website (e.g.,

[18] *See Using HTTP cookies*, MDN Web Docs, (Aug. 23, 2024), https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

[19] *See* ECF No. 97-2, Declaration of Atif Hashmi in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45, at ¶ 8.

buy.avast.com, my.avast.com, and support.avast.com)."[20]

23. It is my understanding that cookies of the type previously installed by Defendant when a user accesses https://www.avast.com (e.g., Google cookies, Meta cookies, etc.) and subsequently transmitted to Defendant's servers can be used by the corresponding third parties to obtain users' browsing data for analytics and other purposes.[21] Furthermore, it is my understanding that data brokers can buy and sell users' browsing data on online advertising exchanges and data marketplaces.[22]

24. For the reasons I have explained above, Plaintiffs' counsel's understanding that Defendant can use AOSP to collect and store users' browsing data and third-party cookie data, and may later transmit it to third parties, has been reasonable from a technological standpoint.

25. Furthermore, for the reasons I will explain below, Defendant has not provided the necessary evidence that would allow me to independently verify that Defendant does not use AOSP to collect and store users' browsing data and third-party cookie data and does not later transmit such data to third parties. Thus, Plaintiffs' counsel's understanding of Defendant's use of AOSP and use of users' browsing data and cookie data remains reasonable from a technological standpoint.

---

[20] Defendant Gen Digital Inc.'s [Corrected] Notice of Motion and Motion for Attorneys' Fees; Memorandum of Points and Authorities in Support Thereof, ECF 140-2 at 6.

[21] *See id.* at ¶ 11; Also *see* ECF No. 97-4, Declaration of Zubair Shafiq in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45.

[22] *See* ECF No. 97-4, Declaration of Zubair Shafiq in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45.

II. Defendant's counsel's August 16 letter did not provide evidence necessary to verify that Defendant does not collect and store AOSP users' cookies and browsing data or transmit AOSP users' data to third parties.

26. It is my understanding that on August 16, 2024, Defendant's counsel sent Plaintiffs' counsel a letter ("Defendant's August 16 Letter") and three documents, which, together, Defendant's counsel asserted offered an explanation for the transmissions and behavior that I observed in my experiments, detailed above and in my prior declaration.[23] The letter provided the same explanation of cookies that Defendant provided in their Motion.[24] Like the explanation in Defendant's Motion, the explanation in the letter sent by Defendant's counsel is incomplete and incorrect for the same reasons I discussed earlier with respect to how browser extensions, including AOSP, can cause the browser to not send cookie data to certain servers.

27. Defendant's August 16 Letter also argued that even if third-party cookies were included in transmissions of AOSP users' browsing data back to Defendant's servers, the three documents accompanying Defendant's August 16 Letter, demonstrate that Defendant "does not do anything with it when it is received by" Defendant's servers.[25] I disagree. The three documents Defendant provided along with Defendant's August 16 Letter are insufficient to support Defendant's conclusion that Defendant's servers do not ingest or utilize AOSP users' cookie data.

28. First, Exhibit A to Defendant's August 16 Letter contains screen captures of a custom search script executed by the Defendant across 4 versions of the Urlite source code

[23] *See* **Exhibit 2**, Aug. 16, 2024, Letter from S. Turner to J. Rotter.
[24] *See id.* at pp. 3-5; *see also* ECF No. 140-2, Defendant's Corrected Notice of Motion and Motion for Attorneys' Fees, pp. 4-8.
[25] *See* **Exhibit 2**, Aug. 16, 2024, Letter from S. Turner to J. Rotter at p. 5.

repository and corresponding search results.[26] These 4 versions are dated 8/6/2021, 6/22/2022, 6/6/2023, and 8/5/2024.[27] The custom search script includes a limited number of search keywords of the form *headers*, *headers.get*, *HEADER_NAME*, *CONTENT_TYPE*, *USER_AGENT*, and *CONTENT_LENGTH*. This means that within the Urlite source code, any source code statements that matches the search keyword and their variations (along with a few lines before and after) are displayed within the search results. Interestingly, the search keywords used by the custom search script do not include the term *COOKIE* or any variations of this term. Thus, I am not surprised to see that the search results do not include any statements that reference the term *COOKIE* or any of its variations. Given that the search results shown in Exhibit A to Defendant's August 16 Letter are obtained by using a limited number of search keywords that were hand-selected by Defendant and, in particular, did not include the keyword *COOKIE* or its variations, these search results are incomplete and are insufficient to conclude that Defendant's servers do not ingest or utilize AOSP users' cookie data. I note that even if the search keywords used by the Defendants include the term COOKIE or its variations, the search results would still be incomplete as within the Urlite source code the term *COOKIE* may be renamed to some other term like *USER_DATA*. Thus, to come to a reasonably certain conclusion that Defendant's servers do not ingest or utilize AOSP users' cookie data, one needs to review the entirety of the Urlite source code and the

[26] A source code repository is a storage location for source code and other software development assets. A source code repository maintains changes made to the source code over time.

[27] Plaintiffs' counsel informed me that the relevant period in this case extends back to December 2020. As such, Defendant did not even search the source code applicable to the first eight months of the relevant period.

source code of any accompanying components in a structured manner to determine if the Urlite and any accompanying components in any way ingest or use users' cookie data.

29. Second, Exhibit B to Defendant's August 16 Letter is a one-page document titled "Data Storing in Urlite Service." This document describes the structure and content of the data that is stored by the Urlite Service whenever there is a hit on a malicious domain. In other words, Exhibit B only relates to the scenario when the URL being analyzed by the Urlite Service matches with a malicious domain. This document does not describe what data is stored by the Urlite Service for the different scenarios where the URLs being analyzed by the Urlite Service do not match a malicious domain. Thus, the discussion in the one-page document titled "Data Storing in Urlite Service" is incomplete and is insufficient to conclude that Defendant's servers do not ingest or utilize AOSP users' cookie data.

30. Third, Exhibit C to Defendant's August 16 Letter is a set of samples stored by the Urlite Service when the URL being analyzed by the Urlite Service matches with a malicious domain. As is the case with Exhibit B to Defendant's August 16 Letter, Exhibit C also only relates to the scenario when the URL being analyzed by the Urlite Service matches with a malicious domain. This document does not describe what data is stored by the Urlite Service for the different scenarios where the URLs being analyzed by the Urlite Service do not match a malicious domain. Thus, the samples stored by the Urlite Service shown in Exhibit C to Defendant's August 16 Letter are incomplete and are insufficient to conclude that Defendant's servers do not ingest or utilize AOSP users' cookie data.

31. To conclusively determine whether or not Defendant used AOSP to collect and store AOSP users' browsing data and third-party cookie data and transmitted that data

to third parties, I would need to review relevant documents and information, including Defendant's server and database schemas for all tables that store AOSP related data and configurations, as well as AOSP's and Urlite's current and historical server—and database—side source code. I understand that to date, Defendant has not provided these materials to Plaintiffs.

32. Because Defendant's August 16 letter and attachments failed to substantiate Defendant's claim that it did not use the cookies it obtained from AOSP users, Plaintiffs' continued pursuit of this case remained reasonable from a technological standpoint even after Defendant's August 16 Letter.

III. Plaintiffs' discovery conduct related to technological issues has been reasonable.

A. Plaintiffs' first set of discovery requests.

33. Based on my review of Plaintiffs' first set of discovery requests and Defendant's responses related to technological issues and objections thereto, I determined that from a technological standpoint those discovery requests were reasonably tailored to seek information necessary to determine whether Defendant used AOSP to collect and store AOSP users' browsing data and third-party cookie data and transmitted such data to third parties.[28]

34. Requests for Production 3-6 sought documents and information about, among other things, the cookies included in transmissions between AOSP and Defendant's servers. Documents and information responsive to these requests can provide details related to

[28] *See* **Exhibit 3**, Plaintiffs' First Set of Requests for Production of Documents to Defendant Gen Digital.

cookie data that was appended to users' browsing data and transmitted to Defendant's servers and can also clarify if Defendant used and/or transmitted the users' browsing data and cookie data to third parties.

35. Requests for Production 7-12 and 16-17 sought information about the transmissions of AOSP user data that Defendant received and transmitted to third parties, as well as technical documentation, source code, any agreements, and other arrangements between Defendant and third parties related to transmission of users' data from Defendant's servers to third parties. Documents and information responsive to these requests can show whether or not Defendant's servers used, stored, and/or transmitted the users' browsing data and cookies data to third parties.

36. Requests for Production 13-15, 18-20, and 28 sought information about Defendant's internal and external uses of the users' browsing data, cookies data, and personal identifiable information, including internal data linking and provision of advertising services. Documents and information responsive to these requests can show the extent to which Defendant used users' browsing data, along with the cookie information, to associate users' online activity with their unique identifiers, categorize users, and whether Defendant transmitted this information to third parties.

37. Requests for Production 21-23 and 27 sought AOSP's source code, as well as Defendant's website, server, and database source code related to AOSP's operations and operations related to receipt of users' browsing data and cookies data, and transmission of this information to third parties, and changes to that source code over time. Documents and information responsive to these requests can show how and what type of information

Defendant collected related to users' browsing data, how Defendant installed or enabled third parties to install cookies within users' browsers and configured the browsers to append cookie data to transmissions sent to Defendant's servers, and whether Defendant stored users' browsing data and cookie data and transmitted it to third parties.

38. Requests for Production 24-26 and 29-34 sought documents, information, and data related to the servers and databases involved in AOSP's operations. Documents and information responsive to these requests can show the extent to which Defendant stored users' browsing data and cookies data and linked users' online activity with unique identifiers. Documents and information responsive to these requests can also show the actual data values related to users that used AOSP along with any cookie related data.

B. Plaintiffs' second set of discovery requests.

39. Based on my review of Plaintiffs' second set of discovery requests and Defendant's responses related to technological issues and objections thereto, I determined that from a technological standpoint those discovery requests were reasonably tailored to seek the information necessary to understand the use of the *credentials* parameter (discussed above) with respect to transmission of cookie data to Defendant's servers.[29]

40. Requests for Production 67-68 sought documents and information related to Defendant's technological requirements and purposes to install cookies within users' browsers and any cross-domain data sharing practices. Documents and information responsive to these requests would have shown why Defendant, from a technological

[29] *See* **Exhibit 4**, Plaintiffs' Second Set of Requests for Production of Documents to Defendant Gen Digital.

standpoint, required first-party or third-party cookies to be installed on users' browsers and whether Defendant engaged in any cross-domain data sharing.

41. Requests for Production 69-71 and 74-77 sought documents and information related to Defendant's configuration of the *credentials* parameter. Documents and information responsive to these requests can show whether AOSP caused the browsers to append cookie data to users' browsing data transmitted to Defendant's servers. (I explained above the importance of the *credentials* parameter and the role it plays in controlling the behavior of web browsers to include or not include cookies in transmissions to servers.)

42. Requests for Production 72-73 sought documents and information related to the configuration of the avast.com domain and the urlite.ff.avast.com subdomain servers. Documents and information responsive to these requests can show whether any of these servers in any way install cookies within users' browsers and configure users' browsers to transmit cookies across domains and subdomains, such that data collected by AOSP would be sent to the urlite.ff.avast.com subdomain.

C. Plaintiffs' third set of discovery requests.

43. Based on my review of Plaintiffs' third set of discovery requests and Defendant's responses related to technological issues and objections thereto, I determined that from a technological standpoint those discovery requests were reasonably tailored to seek the information necessary to understand the use of the *Set-Cookie* header (discussed above) by Defendant, changes in the cookie data transmitted to Defendant's servers, and any

transmissions of data collected using AOSP to services provided by Google, Adobe, and Meta.[30]

44. Requests for Production 80 sought documents and information related to the configuration of the *Set-Cookie* header (discussed earlier) corresponding to third-party cookies. Documents and information responsive to this request can show whether and how Defendant configured the *Set-Cookie* header for various third-party cookies during the relevant period and whether such configurations enabled Defendant to share data across the avast.com domain and other subdomains.

45. Requests for Production 81-86 sought documents and information related to Defendant's use of third-party services provided by Google, including Google Tag Manager. Google Tag Manager is a tag management system provided by Google that allows website developers to set up and manage tags on their websites.[31] Using Google Tag Manager, website developers can send users' browsing data to Google directly from their website (client-to-server model) or from their server (server-to-server model) for analytics and other tracking purposes.[32] Documents and information responsive to these requests can show the extent to which Defendant utilizes Google Tag Manager services and shares users' browsing data and cookies data with Google.

46. Requests for Production 87-95 sought documents and information related to Defendant's use of third-party services provided by Adobe, including Adobe Experience

[30] *See* **Exhibit 5**, Plaintiffs' Second Requests for Production of Documents to Defendant Gen Digital; Also *see* https://support.google.com/tagmanager/answer/6102821?hl=en.
[31] *See* https://support.google.com/tagmanager/answer/6102821?hl=en
[32] *See* ECF No. 97-4, Declaration of Zubair Shafiq in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45. Also *see* https://developers.google.com/tag-platform/tag-manager/server-side/intro.

Cloud, Adobe Experience Cloud ID Service, and Adobe Analytics. Adobe Experience platform includes a set of services that enable organizations to centralize and standardize customer data and content in real-time and apply data science and machine learning to dramatically improve the design and delivery of rich, personalized experiences.[33] Adobe may use this data for tracking purposes.[34] Documents and information responsive to these requests would have shown the extent to which Defendant utilizes Adobe Experience services and shares users' browsing data and cookies data with Adobe.

47. Requests for Production 96-102 sought documents and information related to Defendant's use of third-party services provided by Meta, including Meta Business Tools. Meta Business Tools help website owners and publishers, app developers, and advertisers to integrate and share data with Meta, understand and measure their products and services, and better reach people who use or might be interested in their products and services. Using Meta Business Tools, website developers can send users' browsing data to Meta directly from their website (client-to-server model) or from their server (server-to-server model) for analytics and other tracking purposes.[35] Documents and information responsive to these

[33] *See* https://business.adobe.com/#:~:text=Experience%20Cloud%20lets%20you%20deliver,integrated%20with%20the%20sales%20process.

[34] *See* ECF No. 97-4, Declaration of Zubair Shafiq in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45. Also *see* https://business.adobe.com/products/adobe-analytics.html.

[35] *See* ECF No. 97-4, Declaration of Zubair Shafiq in Support of Plaintiffs' Motion to Compel Compliance with Subpoenas Pursuant to Federal Rule of Civil Procedure 45. Also *see* Nardjes Amieur, et al., Client-side and Server-side Tracking on Meta: Effectiveness and Accuracy, Proceedings on Privacy Enhancing Technologies 2024(3), 431-445 (July 2024), https://petsymposium.org/popets/2024/popets-2024-0086.pdf.

requests would have shown the extent to which Defendant utilizes Meta Business Tools and shares users' browsing data and cookies data with Meta.

D. Plaintiffs' third-party subpoenas.

48. Based on my review of Plaintiffs' Subpoenas to Produce Documents Pursuant Federal Rule of Civil Procedure 45 (the "Subpoenas") directed to non-parties Adobe, Inc., META Platforms Inc., Alphabet, Inc., Reddit, Inc., and Microsoft Corporation (collectively, the "Non-Parties"), and Defendant's objections thereto, I determined that from a technological standpoint the Subpoenas directed to the Non-Parties reasonably sought information relevant to Plaintiffs' theory that Defendant transmitted browsing data and cookies to those third parties.

49. Most importantly, the Subpoenas to the Non-Parties requested all data that the Non-Parties received from Defendant "other than web browsing information from the avast.com website" and all databases, data logs, datasets, and data reports related to the same. Documents and information responsive to these requests can show if the Non-Parties received any data that was transmitted by Defendant from software other than the avast.com website, for example, AOSP. Furthermore, Documents and information responsive to these requests can show the timeline for when data was received by the Non-Parties, and what information was included in that data.

IV. Plaintiffs' discovery request for source code production has been reasonable.

50. Finally, it is my understanding, after reviewing Plaintiffs' latest joint letter with Defendant to the Court that Plaintiffs requested that the Court order Defendant to produce AOSP's and Urlite's current and historical server—and database—side source

code.[36] Because neither Defendant nor the subpoenaed third parties have produced documents or information responsive to Plaintiffs' discovery requests and because the evidence Defendant provided was, from a technical perspective, insufficient and incomplete, Plaintiffs' request for AOSP's and Urlite's current and historical server—and database—side source code review was reasonable and appropriate from a technological standpoint.

51. In the absence of the aforementioned evidence, the only other way for me to assess Defendant's position that Defendant does not use AOSP to collect and store AOSP users' browsing data and third-party cookie data and transmit such data to third parties is to review AOSP's and Urlite's current and historical server—and database—side source code. Reviewing that source code can allow me to, among other things, understand and determine the type of users' browsing data that AOSP collects and transmits to Defendant's servers and any third-party servers, how AOSP configures the browser to append cookie data with users' browsing data in transmissions to Defendant's servers, how the Defendant's servers process and store users' browsing data and cookie data upon receiving the data transmitted by AOSP, and to what extent Defendant's servers transmit users' browsing data and cookie data to third-party servers. Reviewing source code for historical versions can enable me to determine if and how any of the above-mentioned functionalities changed throughout the relevant period. (Oftentimes, such information is not maintained within technical documentation other than source code.)

V. Determining which cookies may have been installed when a user visited avast.com during the relevant period.

[36] *See* ECF No. 116, Plaintiffs' and Defendant Gen Digital's Joint Discovery Letter re: Source Code.

52. It is my understanding that Defendant has not produced any materials responsive to Plaintiffs' Requests for Production 21-23, 24-27, 29-34, and 80. Above, I explained that materials responsive to these requests can show whether and how during the relevant period Defendant configured avast.com website to install third-party cookies on AOSP users' browsers. These materials (if available) can also show the actual user data values received by the Defendant in relation to AOSP, which may further specify the timeline of when those user data values were received along with any cookies data. Using this information (if available), both Defendant and Plaintiffs can determine which cookies would have been installed on the devices of the users who visited avast.com website during the relevant period.

VI. Absence of on-device cookie data is not determinative of whether the subject cookies were present or absent from Plaintiffs' devices at various points in time.

53. Because of the nature of cookie data, the presence or absence of the subject cookies on the Plaintiffs' devices at the time when the devices were imaged and the corresponding creation and modification dates are not determinative of the presence or absence of the subject cookies at various points in time during the relevant time period in this case.

54. Oftentimes, cookies installed within a browser include an expiration date or an expiration period.[37] If a cookie is not renewed before its expiration date or expiration period, the browser automatically deletes the cookie.[38] Cookies can also be deleted

[37] *See* https://developer.chrome.com/blog/cookie-max-age-expires; Also *see* https://learn.microsoft.com/en-us/dotnet/api/system.net.cookie.expires?view=net-8.0; Also *see* https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

[38] *See* https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

automatically based on browser settings,[39] or by deletion of browsing history. When browsing history is deleted, cookie data stored by the browser is also deleted. Subsequently, when the cookies are re-installed, the creation and modification dates associated with the cookie may change.

55. Thus, for the reasons discussed above, the presence or absence of the subject cookies on the Plaintiffs' devices at the time they were searched is not determinative of whether the subject cookies were present or absent from Plaintiffs' devices at various points in time during the relevant period. Furthermore, as discussed earlier, using historical versions of configurations for avast.com website related to installing cookies on AOSP users' browsers (if available), Defendant can determine which cookies would have been installed on the devices of the users who visited avast.com website during the relevant period.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed November 20, 2024, in Prosper, Texas.

Atif Hashmi

[39] *See* https://support.google.com/chrome/community-guide/245444314/how-to-automatically-clear-browsing-data-when-closing-google-chrome-window-a-step-by-step-guide?hl=en